

Payment Card Industry Data Security Standard (PCI DSS) 4.0 Implementer

- Learn how to minimize the possibility of card breach, improve security, reduce the risk of data losses.
- Acquire knowledge on functioning of Payment Card Industry and the transaction flows.
- Understand what Cardholder Data and Sensitive Authentication Data and risk is associated with same.
- Comprehend the complete PCI DSS compliance process and make informed decisions regarding compliance efforts

What will you learn?

With the help of PCI DSS training, you will understand the various requirements of the Payment Card Industry Standards and learn the intent behind each of its requirements. If your organisation is already PCI compliant, the PCI DSS training and implementation workshop will help you learn how to maintain your PCI-compliant status effectively and minimise the possibility of card breaches, resulting in a secure PCI environment.

Course outline

- Acquire knowledge on functioning of Payment Card Industry and the transaction flows.
- Be acquainted with the roles and responsibilities of various organizations in the Payment Card Industry and figure out different standards for different organizations.
- Understand what Cardholder Data and Sensitive Authentication Data and risk are associated with same.
- Learn how to minimize the possibility of card breach, improve security, reduce the risk of data losses.
- Gaining a thorough understanding of the intent behind each requirement.
- Comprehend the complete PCI DSS compliance process and make informed decisions regarding compliance efforts.

- Learn about Merchants and Service Provider Levels and their Compliance requirements.

Note: Exercises, assignments, group discussions, and case studies will be spread across all days

Who Should Attend?

- Managers overseeing PCI DSS compliance
- External auditors performing PCI DSS validation
- Security professionals operating in a PCI DSS compliant environment
- Internal auditors desiring to validate interim compliance
- IT staff, project managers & Risk Managers

Pre-requisites

- Understand the Plan-Do-Check-Act (PDCA) cycle.
- Roles and responsibilities as cyber security personnel.
- Incorporating management commitment and the interests of stakeholders.
- Enhancing societal values.
- Incorporating security as an essential element of information networks and systems.
- Active prevention and detection of Risk incidents.
- Ensuring a comprehensive approach to Risk management.
- Continual reassessment of Risk and making of modifications as appropriate.

Learning & Career benefits

- Enhanced Data Security
- Compliance with Regulatory and Industry Standards
- Builds Customer Trust
- Business Continuity and Risk Management
- Financial Benefits
- Competitive Advantage
- Ongoing Security and Continuous Improvement
- Streamlined Business Operations
- Preparation for PCI DSS Audits

Examination & Certification

- Online web proctored based.
- 40 Multiple choice questions 1 mark each.
- Total marks: 40
- Passing criteria: 70% (28 out of 40 marks) to pass.
- Duration: 60 minutes

Note:

- The course material and the notes can be referred to during the exam.
- You must have access to a clean, unmarked copy of the relevant PCI DSS standard.

Certification

- Only candidates who successfully passes the examination will be awarded TÜV SÜD's Certified PCI DSS implementer certificate.
- Candidates who do not pass the examination may retake it.